# EXHIBIT 1

P1

FILED
JUN 09 2010
DAVID H. YAMASAKI
Clerk of the Superior Court of Santa Clara
By C. Mendoza Deputy

CSW 39460

STATE OF CALIFORNIA – COUNTY OF SANTA CLARA, SW No.

# RETURN TO SEARCH WARRANT

Ofc. Daniel Ichige #3365 San Jose Police Department, being sworn, says that he/she (conducted a search pursuant to the below described search warrant:
Issuing magistrate: The Honorable Judge Paul Teilh
Superior Court, County of Santa Clara
Date of Issuance: June 2, 2010
Date of Service: June 2, 2010
and searched the following location(s), vehicle(s), person(s):

SBC Internet Services, 1010 N.St.Mary's St. Rm. 315-A2, San Antonio, TX 78215

and seized the items*:
_____described in the attached and incorporated inventory.
__X__described below:

Six pages of documents

I further swear that this is a true and detailed account of all the property taken by me pursuant to the search warrant, and that pursuant to Penal Code sections 1528 and 1536 this property will be retained in my custody, subject to the order of this court or any other court in which the offense in respect to which the seized property is triable.

Ichin 3365
(Signature of Affiant)

**Sworn to and subscribed before me this** 9th **day of** June, 2010.

Paul R Teilh
(Signature of Magistrate)
Judge of the Superior Court, County of Santa Clara
PAUL R. TEILH

*List all items seized, including those not listed on the search warrant.
(revised 12-03-08)

THE FOREGOING INSTRUMENT IS A CORRECT COPY OF THE ORIGINAL ON FILE IN THIS OFFICE
ATTEST: DAVID H. YAMASAKI
JUN 09 2010
CHIEF EXECUTIVE OFFICER/CLERK
SUPERIOR COURT OF CA COUNTY OF SANTA CLARA
IN AND FOR THE COUNTY OF SANTA CLARA
BY _____ DEPUTY

STATE OF CALIFORNIA - COUNTY OF SANTA CLARA, SW NO. _____

# SEARCH WARRANT

FILED
JUN 09 2010
DAVID H. YAMASAKI
Chief Executive Officer/Clerk
Sup. Ct. of Ca County of Santa Clara
DEPUTY

CSW 39460

THE PEOPLE OF THE STATE OF CALIFORNIA TO ANY PEACE OFFICER IN THE COUNTY OF SANTA CLARA:

Proof by affidavit and under penalty of perjury having been sworn to this day before me by
**Ofc.Daniel Ichige #3365 San Jose Police Department**
that there is probable cause for believing that the property and/or person described below may be found at the location(s) set forth below and is lawfully seizable pursuant to Penal Code Section 1524 as indicated below by "x"(s) in that it:

____ was stolen or embezzled
____ was used as the means of committing a felony
____ is possessed by a person with the intent to use it as means of committing a public offense or is possessed by another to whom he or she may have delivered it for the purpose of concealing it or preventing its discovery
__X__ tends to show that a felony has been committed or that a particular person has committed a felony
__X__ tends to show that sexual exploitation of a child, in violation of Penal Code Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring
____ there is a warrant to arrest the person;

YOU ARE THEREFORE COMMANDED TO SEARCH:

SBC Internet Services, 1010 N.St.Mary's St. Rm. 315-A2, San Antonio, TX 78215

FOR THE FOLLOWING PROPERTY/PERSON:

1. **Any and all information for the following IP addresses with the corresponding dates and times of use:**

| IP Address | Date | Time |
|---|---|---|
| 99.173.27.101 | 05-29-2010 | 20:54:15-0700 UTC |
| 99.173.27.101 | 05-31-2010 | 11:48:46-0700 UTC |

**to include, but not limited to, all subscriber information, such as name, address, phone number, date of birth, gender, date account created, account status, identifying information related to payment method and type, associated e-mail addresses, date ID registered, length of time IP address assigned to subscriber, and MAC address.**

AND TO SEIZE IT/THEM IF FOUND and bring it/them forthwith before me, or this court, at the courthouse of this court. This Search Warrant and incorporated Affidavit was sworn to as true before me this 2d day of June, 20 10, at 4:15 AM. / P.M. Wherefore, I find probable cause for the issuance of this Search Warrant and do issue it.

HOBBS SEALING APPROVED: YES [ ] NO [ ]
NIGHT SEARCH APPROVED: YES [ ] NO [ ]

Paul R Teilh
[Signature of Magistrate]
Judge of the Superior Court, County of Santa Clara
(revised 12-10-08) D#_____ PAUL R. TEILH

CSW39460

STATE OF CALIFORNIA - COUNTY OF SANTA CLARA, SW NO.

FILED
JUN 09 2010
DAVID H. YAMASAKI
Chief Executive Officer/Clerk
Superior Court of CA County of Santa Clara
BY DEPUTY

# AFFIDAVIT

Ofc.Daniel Ichige #3365 San Jose Police Department .....
swears under penalty of perjury that the facts expressed by him/her in the attached and incorporated **Statement of Probable Cause** are true and that based thereon he/she has probable cause for believing and does believe that the **PROPERTY/PERSON TO BE SEIZED**, described below, is lawfully seizable pursuant to Penal Code Section 1524, in that:

____ it was stolen or embezzled
____ It was used as the means of committing a felony
____ It is possessed by a person with the intent to use it as means of committing a public offense or is possessed by another to whom he or she may have delivered it for the purpose of concealing it or preventing its discovery
_X_ It tends to show that a felony has been committed or that a particular person has committed a felony
_X_ It tends to show that sexual exploitation of a child, in violation of Penal Code Section 311.3, or possession of matter depicting sexual conduct of a person under the age of 18 years, in violation of Section 311.11, has occurred or is occurring
____ there is a warrant to arrest the person;

and is now located at
THE FOLLOWING PREMISES AND LOCATION(S):

SBC Internet Services, 1010 N.St.Mary's St. Rm. 315-A2, San Antonio, TX 78215

PROPERTY/PERSON TO BE SEIZED:

1. **Any and all information for the following IP addresses with the corresponding dates and times of use:**

| IP Address | Date | Time |
|---|---|---|
| 99.173.27.101 | 05-29-2010 | 20:54:15-0700 UTC |
| 99.173.27.101 | 05-31-2010 | 11:48:46-0700 UTC |

**to include, but not limited to, all subscriber information, such as name, address, phone number, date of birth, gender, date account created, account status, identifying information related to payment method and type, associated e-mail addresses, date ID registered, length of time IP address assigned to subscriber, and MAC address.**

Wherefore, he/she requests that this Search Warrant be issued.
NIGHT SEARCH REQUESTED: YES [ ] NO [ ]; HOBBS SEALING REQUESTED: YES [ ] NO [ ]

Ichige 3365

[Signature(s) of Affiant(s)]
(revised 12-10-08) D#_____

Your Affiant, Daniel Ichige, is a Police Detective employed by the San Jose Police Department, in San Jose, California. Your Affiant has been a law enforcement officer in the State of California since 1990.

Your Affiant has received the following training in Child Pornography, Child Sexual Exploitation, Child Molest Investigations and Sexual Assault investigations

1990
Basic Academy
Evergreen Valley College Police Academy
San Jose, CA
(24 hours) = Sexual Assault Investigation

2005
Homicide Investigation Course
San Jose State University
San Jose,CA
(40 hours)

2006
Child Death Investigation
Santa Clara County Sheriff's Department
Gilroy,CA
(8 hours)

2009
Internet Crimes Against Children Conference
Department of Justice
San Jose, CA
(32 hours)

2009
Sexual Assault Investigation Course
San Jose State University
San Jose, CA
(40 hours)

2009
ICAC Investigative Techniques
Fox Valley College
Denver, CO
(32 hours)

2010
ICAC Undercover Chat Investigations
Fox Valley College
San Francisco, CA
(32 hours)

2010
Peer to Peer Investigations
Fox Valley College
San Jose, CA
(32 hours)

Summary of Facts:

Your Affiant has been assigned as an investigator in the Child Exploitation Detail of the San Jose Police Department's Sexual Assault Unit since March 2009. Your Affiant has personally arrested or assisted in arresting over 20 sexual offenders and has had the occasion to interview several sexual offenders including child sexual predators. Your Affiant has studied and is familiar with materials relating to the field of Sexual Assault Investigation, Child Pornography, and Child Sexual Exploitation.

Your affiant is being assisted by other members of the San Jose Police Department's ICAC Task Force. Your affiant is currently investigating violations of California Penal Code Section **311.11(a) - Possession of child pornography.**

Nationwide, ICAC Agents began working an Internet undercover operation to identify persons using peer-to-peer (P2P) software on the Internet to traffic in child pornography. Your Affiant knows from training and experience that peer-to-peer networks are frequently used in the trading of child pornography.

While examining P2P file sharing networks, your Affiant learned that computer users can choose to install publicly available software that facilitates the trading of images. The software, when installed, allows the user to search for pictures, movies and other digital files by entering text as search terms. That text search is sent to an ultra-peer. An ultra-peer is an index server that handles requests and examines submitted file lists from peers that it knows about for files matching the text search request. A file list is then sent back to the requesting user who can choose to download files from peers who possess at least a portion of the file.

Your Affiant knows from training and experience that search results presented to the user allow the user to select a file and then receive that file from other users around the world. These users allow the users to select a file and then receive that file from other users around the world. These users can receive the selected file from numerous sources at once. The software can balance the network load and recover from network failures by accepting pieces of the file from different users and then reassembling the file on the local computer.

Your Affiant knows that P2P networks can only succeed in reassembling the file from different parts if the parts all come from the same original file. Your Affiant knows that multiple persons sharing one file can deliver different pieces of that file to the local software and the local software can insure that a complete and exact copy can be made from the parts. Your Affiant has been able to confirm from use of the software that different copies of the same file can be named differently.

Your Affiant knows that P2P computer software has different methods to insure that two files are exactly the same. Your Affiant knows from training and experience that the method used by the P2P Operation described herein involves a compressed digital representation method called Secure Hash Algorithm Version 1 or SHA1. Your Affiant knows that the Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard.

Your Affiant knows that digital files can be processed by this SHA1 standard resulting in a digital signature. By comparing these signatures, your Affiant can conclude that two files are or are not identical with a precision that greatly exceeds 99.9999 percent certainty. Your Affiant knows through the computer forensic community that there has never been a documented occurrence of two different files being found on the Internet having different contents while sharing the same SHA! Value.

Your Affiant knows that the use of SHA1 compressed digital representations for the matching of movies and images has proven to be extremely reliable. Through this method of comparison, your Affiant has matched thousands of files and has never found two files with different contents but the same SHA1 value.

Your Affiant knows from training that the P2P network investigated in this operation uses the SHA1 digital signature to verify the unique identity of individual files. Your Affiant knows that users attempting to trade files on a P2P file sharing network can place files from their local computer in a shared file directory. If that user then starts the P2P software that local computer calculates the SHA1 signature for each shared file and provides that information to other users wishing to trade files.

Your Affiant knows that entering search terms in the P2P software results in a list of SHA1 digital signatures that your Affiant can choose for download. By using this type of search, your Affiant compares the offered SHA1 signatures with SHA1 signatures known to belong to movies or images of child pornography. Your Affiant confirms these SHA1 values as belonging to child pornography by examining the files from previous investigations with the matching SHA1 value. By watching these movies or viewing these image, your Affiant is able to determine the exact file referenced by the given SHA1 value. Once a matching set of digital signatures is identified, your Affiant submits a download request for the file.

This method has proven to be extremely reliable, working just like software used by end users around the world in locating and downloading precise files. Once the download of child pornography is initiated, your Affiant receives a list of download candidates that are participating in the possession, receipt and/or distribution of child pornography. This feature allows your Affiant to conduct undercover operations that involve images of child sexual abuse being traded on peer-to-peer networks.

Your Affiant knows from training and experience that Internet computers identify each other by an Internet Protocol or IP address. Your Affiant knows that IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses lead the law enforcement officer to a particular Internet service provider or company (ISP). Given the date and time the IP address was used, an ISP can typically identify the account holder by name and physical address.

Your Affiant learned that searching on a peer-to-peer network as described above results in your Affiant receiving a list of IP addresses identifying locations where a computer has P2P software installed and individual files have been reported as available for download with a specific digital signature (SHA1).

These computers are referred to as a download candidate. A download candidate is a computer that was reported by an ultra-peer as a source for the file listed by SHA1 value. In almost every known case the download candidate serves those files to P2P users across the Internet.

Computers from throughout the world can download files from download candidates without regard to geographic location. Your Affiant knows that the files located on P2P download candidates are quickly available throughout the world due to the distributed sharing model of P2P networks.

Your Affiant knows the P2P software may display the Globally Unique Identifier (GUID) identification number of computers offering to share files on the network. A Globally Unique Identifier or GUID is a pseudo random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your Affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

Your Affiant knows that cooperating police agencies pool their information to assist in identifying criminal conduct and build probable cause to further criminal investigations. With this pooled information, police get a better understanding of the global information available about a suspect that resides in their area of jurisdiction. This information is valuable when trying to regionalize a suspect to a certain jurisdiction, given the global scope of the Internet. Investigators from around the world gather and log information which can be used by an investigator to build probable cause on one specific case.

Your Affiant has learned that by examining a list of IP addresses your Affiant can locate computers that are reported to be in California. By comparison of the SHA1 digital signatures, your Affiant can conclude that a computer, originating from an IP address known to be in California has P2P software installed on it and contains images of child pornography. With this information, a request can be made to the Internet service provider to identify the specific physical address related to the use of P2P software in the exchange of child pornography.

## Current Investigation

On May 29, 2010, your Affiant was investigating California computers that were sharing child pornography on the Internet. Your Affiant was looking for the offenders actively sharing child pornography within California, specifically in San Jose.

Your Affiant identified IP address 99.173.27.101 as a computer advertising files with titles indicative of child pornography. Following are two examples of the filenames reported:

- Stickam - 13y & 14y Lesbian Jailbaits - [27m41sec].avi
- real video of a 12yo girl taking her bikini off and drying off! Nice little nipples! New 2009 pthc ptsc R@ygold.avi

Your Affiant knows that filenames do not always accurately depict the contents of the file. So, your Affiant selected two of the files offered by IP address 99.173.27.101 to download. I was able to successfully conduct a single-source download of the following files from IP 99.173.27.101 directly to my computer.

**May 29, 2010**
**S3Z4UT5OE3C7EXEBKGIVFNPJB445XGV5**
jailbait-12chan-stickam-hairbrush-mast-ohjosh-anal-moaning-innocent-face.avi
This is a color video file that depicts a completely nude girl in a bathroom. She appears to be approx. 12-15 years old with visible pubic hair and breast development. The video seems to be self produced and depicts the girl masturbating with a hairbrush.

**May 31, 2010**
**UV5GNVW3YFNYS4AAXWJD3DIDCRZ24NYH**
**Webcam - Danielle 12yo and friend shows us all (Hussyfan ptsc pthc).mpg**
This is a color video file that is 21 seconds long. It depicts a girl who is approx. seven to ten years old who is depicted pulling her pants down exposing her buttocks and crotch where no pubic hair is visible. She then pulls her shirt up exposing her chest which displays hardly any breast development.

After I determined that the files were in fact child pornography, I was able to determine that the user associated with IP address **99.173.27.101** was involved with the receiving, possessing, and/or distributing of child pornography. The connection was established on **May 29, 2010** at approx **20:54:15-0700 UTC** hours.

An internet search revealed that IP address 99.173.27.101 is registered to SBC Internet Services.

Your Affiant, by virtue of his training and experience, knows that Internet Service Providers maintain, log, and store account information for subscribers which can include but not be limited to e-mail accounts, IP history related to session dates & times, online digital storage, etc.. Your affiant believes that SBC Internet Services is in possession of the above requested information. The above subscriber information will assist in identifying the primary suspect.

Your Affiant therefore believes that evidence of the commission of Felonies and items used in the commission of Felonies, to wit: violation of California Penal Code section **311.11(a)-Possession of child pornography,** will be located where described above. Based upon the above facts, I request that a daytime search warrant be issued for the above location(s) for the seizure of said property and that the same be held under California Penal Code § 1536 and disposed of according to law.

THE FOREGOING INSTRUMENT IS
A CORRECT COPY OF THE ORIGINAL
ON FILE IN THIS OFFICE
ATTEST: DAVID H. YAMASAKI

JUN 09 2010

CHIEF EXECUTIVE OFFICER/CLERK
SUPERIOR COURT OF CA COUNTY OF SANTA CLARA
IN AND FOR THE COUNTY OF SANTA CLARA
BY _____ DEPUTY

THE GREAT SEAL OF THE STATE OF CALIFORNIA

TRANSMISSION VERIFICATION REPORT

TIME : 11/24/2010 16:11
NAME :
FAX : 4089719[illegible]4
TEL :
SER.# : BROF7J6[illegible]072

| | |
|---|---|
| DATE,TIME | 11/24 16:08 |
| FAX NO./NAME | 19256461389 |
| DURATION | 00:02:36 |
| PAGE(S) | 12 |
| RESULT | OK |
| MODE | STANDARD ECM |

## IP Assignment Details

| Date & Time (GMT) | Record Type | Username | Assigned IP |
|---|---|---|---|
| 05/29/2010 22:11:03 | Start | abursch@sbcglobal.net | 99.173.27.101 |
| 05/30/2010 05:26:49 | Stop | abursch@sbcglobal.net | 99.173.27.101 |
| | | | |
| 05/31/2010 16:23:58 | Start | anacarino25@att.net | 99.173.27.101 |
| 05/31/2010 21:44:18 | Stop | anacarino25@att.net | 99.173.27.101 |

## Customer Account Details

Customer Name
ALEX BURSCH

Account Number
32505487

Member ID's

| Master | Member ID | Domain | Service Status | Portal Provider | Portal Effective Date |
|---|---|---|---|---|---|
| ✓ | abursch | sbcglobal.net | Active | AT&T Yahoo | 09/06/2008 |

Customer Name
ALEX BURSCH

Account Number
32505487

Account Details

| | | | | | |
|---|---|---|---|---|---|
| Account Status: | Active | Reason Code: | | | |
| Prev Account: | | Region: | PBI | BUS/RES: | Res |
| Billing Start Date: | 09/04/2008 | Billing End Date: | | Bill Round: | 4 |
| Tax Exemption | ☐ | Tax ID: | | Exemt Exp: | |

Get Eligible Discounts

Payment Method

BTN BTN: (925) 765-9449 Cust Code: 000

Credit Card
Credit Card Type:
Card Number's Last Four Digits:
Expiration Month:
Card Expiration Year:

Invoice

Change Payment Details

Billing Address

*Description: Individual Consumer

Address Summary

| Primary | Address | Start Date | End Date | |
|---|---|---|---|---|
| ☑ | 5016 WAGON WHEEL WY Antioch CA 94509 USA | 09/03/2008 | | Edit |

| Installed Service ID | Description | Customer |
|---|---|---|
| 161248780 | DSL Dynamic IP | ALEX BURSCH |

**Customer Information**

| | | | |
|---|---|---|---|
| Customer: | BURSCH,ALEX | Address | |
| Member ID: | abursch | Status: | Activated |
| Domain: | sbcglobal.net | WTN: | (925) 765-8449 |
| Order ID: | 121902450 | | |
| Account Number: | 32505487 | Account Status: | Active |

**ProdHist Information**

Product ID: [redacted] DSL Dynamic IP

Order Taken Date: 08/29/2008

Service Activation Date: 09/04/2008 12:00:00AM

Service Deactivation Date:

**[redacted]**

Date Registered: 09/05/2008

## Service Address

First Name: ALEX Last Name: BURSCH

Company:

Address1: 5018 WAGON WHEEL WY

Address2:

Address3:

City: ANT

State: CA California Zip: 94509

Connection records on or before 3/30/09 are logged in Eastern and adjust during Daylight Saving.
Connection records on or after 3/31/09 are in GMT/UTC.

# IP Assignment Details

| Date & Time (GMT) | Status | Username | Assigned IP |
|---|---|---|---|
| 06/01/2010 14:18:10 | Stop | abursch@sbcglobal.net | 99.173.27.152 |
| 05/31/2010 17:27:49 | Start | abursch@sbcglobal.net | 99.173.27.152 |

# Customer Account Details

**Customer Name**
ALEX BURSCH

**Account Number**
32505487

**Account Details**

| | | | | | |
|---|---|---|---|---|---|
| **Account Status:** | Active | **Reason Code:** | | | |
| **Prev Account:** | | **Region:** | PBI | **BUS/RES:** | Res |
| **Billing Start Date:** | 09/04/2008 | **Billing End Date:** | | **Bill Round:** | 4 |
| **Tax Exemption** | ☐ | **Tax ID:** | | **Exem Exp:** | |

Get Eligible Discounts

**Payment Method**

◉ **BTN** **BTN:** (925) 755-8448 **Cust Code:** 000

○ **Credit Card**
**Credit Card Type:** **Card Number's Last Four Digits:**
**Expiration Month:** **Card Expiration Year:**

○ **Invoice**

Change Payment Details

**Billing Address**

Connection records on or before 3/30/09 are logged in Eastern and adjust during Daylight Saving.
Connection records on or after 3/31/09 are in GMT/UTC.

| Installed Service ID | Description | Customer |
|---|---|---|
| 151248780 | DSL Dynamic IP | ALEX BURSCH |

**Customer Information**

| | | | |
|---|---|---|---|
| **Customer:** | BURSCH,ALEX | Address | |
| **Member ID:** | abursch | **Status:** | Activated |
| **Domain:** | sbcglobal.net | **WTN:** | (925) 755-8449 |
| **Order ID:** | 121802450 | | |
| **Account Number:** | 32505487 | **Account Status:** | Active |

**Product Information**

| | | | |
|---|---|---|---|
| **Product ID:** | [illegible] | DSL Dynamic IP | |
| **Order Taken Date:** | 08/28/2008 | **Service Activation Date:** | 09/04/2008 12:00:00AM |
| | | **Service Deactivation Date:** | |

**Registration**

**Date Registered:** 09/06/2008

**Service Address**

| | | | |
|---|---|---|---|
| First Name: | ALEX | Last Name: | BURSCH |
| Company: | | | |
| Address1: | 5016 WAGON WHEEL WY | | |
| Address2: | | | |
| Address3: | | | |
| City: | ANT | | |
| State: | CA California | Zip: | 94509 |

Connection records on or before 3/30/09 are logged in Eastern and adjust during Daylight Saving.
Connection records on or after 3/31/09 are in GMT/UTC.

# Business Records Certification

I, **Chris Bader**, the undersigned, hereby declare:

1. I am a United States citizen and over eighteen years of age.

2. I am employed by AT&T as Internet Legal Compliance Manager. My job responsibilities include retrieving AT&T Internet Services records responsive to legal process for such records.

3. AT&T was served with legal process for business records described there in. A copy of the legal process is attached.

4. The following are responsive:
   a) Attached hereto is a true copy of the available records described in the legal process.
   b) Attached hereto is a true copy of the results of our search, assembly, and production.

5. I affirm these records:
   a) were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
   b) were kept in the course of the regularly conducted activity; and
   c) were made by the regularly conducted activity as a regular practice.

This declaration was made in the State of Georgia and I affirm, under penalty of perjury, that the foregoing is true and correct.

Executed on 7/22/2010

Chris Bader

**Chris Bader**
Manager, Internet Legal Compliance
AT&T Internet Services
575 Morosgo Drive NE, Suite 5D43
Atlanta, GA 30324
404-499-5211

| REPORT TYPE | SJPD - SAIU SUPPLEMENTARY REPORT | CASE NUMBER |
|---|---|---|
| Possession of Child Pornography | | 10-149-9710 |

**Narrative:**

At the time of this report I was working as a Detective in the Sexual Assaults Investigations Unit. I was assigned specifically to the Child Exploitation Detail/ Internet Crimes Against Children Task Force.

The purpose of this supplemental report is to confirm and authenticate the application of a search warrant for subscriber information relating to IP address 99.173.27.101. I prepared a search warrant directing SBC Internet Services to provide subscriber information relating to this IP address. I presented this search warrant to The Honorable Judge Paul Thiel of The Santa Clara County Superior Court and he signed it.

I served the search warrant with SBC Internet Services and they provided me with the following information:

Alex Bursch

5016 Wagon Wheel Way

Antioch, California 94509

No further.

| OFFICER'S NAME | ID NUMBER | DATE | SHIFT/DAYS OFF | SUPERVISOR REVIEW | ID NUMBER | DATE | |
|---|---|---|---|---|---|---|---|
| Ichige | 3365 | 3/3/2012 | 1-SSM | | | | PG 1 OF 1 |